

Pôle veille, analyse et prospective

FLASH VIGIOLYMPIQUE RISQUES ET MENACES

Flash n°02 - mercredi 15 mai 2024

Les menaces cyber



HAUT COMITÉ
FRANÇAIS
POUR LA
RÉSILIENCE
NATIONALE



Les prochains flashes*

- **22 mai** – l'activisme violent ;
- **29 mai** – le risque épidémique ;
- **5 juin** – la désinformation ;

* Diffusés chaque mercredi sur notre page LinkedIn à partir du 08.05.24

Haut Comité Français pour la Résilience Nationale

Pôle veille, analyse et prospective

benjamin.roman@team-hcfdc.org

HCFRN 2024 – tous droits réservés

Description des faits

Les Jeux Olympiques et Paralympiques 2024 constituent un enjeu majeur en matière de cybersécurité. Enjeu exacerbé compte tenu du **contexte géopolitique** actuel, de la **médiatisation hors norme** de l'événement et de la **surface d'attaque étendue**. Hacktivistes et groupes APT (*advanced persistent threat* - groupes soutenus par des puissances belliqueuses) ont déjà mené des opérations contre la France. Le 2 mars dernier, et bien que cela se soit soldé par un échec, les hackers du groupe russe *Sandworm* ont ciblé et piraté le réseau d'un moulin (qu'ils prenaient pour une centrale hydroélectrique) et ont abaissé le niveau d'eau de 20 cm¹.

¹ <https://www.zdnet.fr/actualites/moulin-ou-barrage-hydroelectrique-les-pirates-russes-de-sandworm-semmelent-les-pinceaux-390797.htm>

Haut Comité Français pour la Résilience Nationale

Pôle veille, analyse et prospective

benjamin.roman@team-hcfdc.org

HCFRN 2024 – tous droits réservés

Mise en contexte

Ces dernières années, les **grands évènements sportifs internationaux** ont représenté des cibles de choix pour les cyberattaques d'ampleur. L'exclusion renouvelée de l'équipe olympique russe des jeux de Paris pourrait motiver le Kremlin à perpétrer des attaques informatiques élaborées et cherchant à entraver le bon déroulé des Jeux. En 2018, la cérémonie d'ouverture des Jeux d'hiver en Corée du Sud avait déjà fait l'objet d'un **sabotage informatique** conduit par le GRU russe, via le virus *wiper Olympic Destroyer*. De même, les services de renseignement britanniques ont révélé fin 2020 l'existence d'opérations visant les Jeux de Tokyo. **Une attaque sur la chaîne d'approvisionnement** visant le prestataire Fujitsu avait été perpétrée par un groupe APT chinois. Les **rançongiciels** et la **déstabilisation** via des attaques de type DDoS, sont également des moyens d'action auxquels les hackers peuvent recourir pour **porter atteinte à l'organisation des Jeux**.

Haut Comité Français pour la Résilience Nationale

Pôle veille, analyse et prospective

benjamin.roman@team-hcfdc.org

HCFRN 2024 – tous droits réservés

Perspectives

Pour les Jeux de Paris 2024, les prises de position françaises dans le contexte géopolitique actuel peuvent favoriser une recrudescence du nombre d'attaques par des puissances étrangères hostiles. Celles-ci seraient facilitées par l'**interconnexion des systèmes d'information** des différentes structures organisatrices. Cette large surface d'attaque, associée à une préparation parfois insuffisante de ces quelques centaines d'entités identifiées font craindre à une multiplication des cyberattaques. Pour autant, si l'**ANSSI** et le TOC¹ ont procédé à un durcissement des **réseaux critiques**, on peut s'attendre à des attaques de type DDoS visant les écrans de rediffusion ou les systèmes de chronométrage, qui, combinés à une campagne de communication, pourrait voir l'effet recherché exacerbé. La criticité des attaques sera d'autant plus importante que les Jeux ne s'étendent que sur une courte période, concentrant de fait un nombre très important d'**offensives malveillantes** sur les deux semaines de compétition.

¹ Technology Operations Center

Haut Comité Français pour la Résilience Nationale

Pôle veille, analyse et prospective

benjamin.roman@team-hcfdc.org

HCFRN 2024 – tous droits réservés

Haut Comité Français pour la Résilience Nationale

Association loi 1901 reconnue d'intérêt générale

Informations

Hugo Fiora : délégué général adjoint

hugo.fiora@team-hcfdc.org - 06 45 86 51 60

Pôle veille, analyse et prospective – mission VigiOlympique 2024

Contact

Benjamin ROMAN : responsable du pôle

benjamin.roman@team-hcfdc.org - 01 89 96 09 05



↗ hcfrn.org